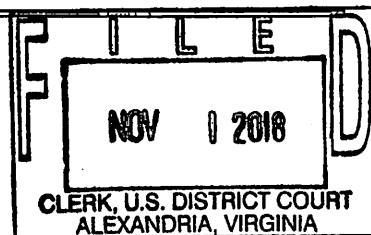


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Two Cell Phones and SIM Cards located at
1800 N. Kent street, Arlington VA

Case No. 1:18-sw-659

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Two iPhone cellular phones and two SIM cards contained therein, secured at the office at Diplomatic Security Service's Office of Special Investigations, 1800 N. Kent street, Arlington VA, as described in Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See attachment B incorporated herein and included as part of the Affidavit in Support of this Application for a Search Warrant

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 USC 1111

18 USC 7(9)

Murder

Special Maritime and Territorial Jurisdiction

Offense Description

The application is based on these facts:
See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kenneth K. Jones, Special Agent, DSS

Printed name and title

Sworn to before me and signed in my presence.

Date: 1 Nov 18

City and state: Alexandria, VA

/s/

Ivan D. Davis

United States Magistrate Judge

ATTACHMENT A

The property to be searched are two cell phones and the SIM cards located within each, collectively, “the Devices”:

- a. An Apple iPhone 6S, Model A1633, FCC ID BCG-E2946A bearing a sticker barcode with the number 027411, hereinafter Device 1. The phone’s serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369250. The protective case of the phone bears a sticker with the number 034 49 352 10. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.
- b. An Apple iPhone 7, Model A1660, FCC ID BCG-E3085A, hereinafter Device 2. The phone’s serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369235. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

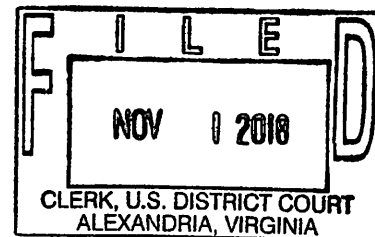
All records on the Devices described in Attachment A that relate to the victim, Kevin Webb's activities, whereabouts, and communications preceding his death, including:

- a. Any Device application that facilitates communication, particularly translated communication;
- b. any archived information related to Mr. Webb's location as recorded by the Devices' GPS;
- c. any information, such as contact information, demonstrating the nature of the relationship between Mr. Webb and the subject of investigation;
- d. any Device media which, with time-stamps, correlate Mr. Webb's location and activities in the hours preceding his death; and
- e. evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION



IN THE MATTER OF THE SEARCH OF
TWO CELL PHONES AND SIM CARDS
CURRENTLY LOCATED AT 1800 N. KENT
STREET, ARLINGTON, VIRGINIA

Case. No. 1:18-sw-659

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR
AWARRANT TO SEARCH AND SEIZE**

I, Kenneth K. Jones, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two Apple iPhones and the SIM cards contained therein—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Diplomatic Security Service (DSS) and have been since 2007. I hold an M.S. in forensic science, with an emphasis in computer forensics, from the Marshall University Forensic Science Center. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program.

3. I am currently assigned to the Office of Special Investigations, where my responsibilities include investigating certain violent crimes occurring overseas, including murder of U.S. embassy personnel abroad.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched are two wireless phones and the subscriber identity module (SIM) cards located within each, hereafter collectively, "the Devices":

- a. An Apple iPhone 6S, Model A1633, bearing a sticker barcode with the number 027411, hereinafter "Device 1." The phone's serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369250. The protective case of the phone bears a sticker with the number 034 49 352 10. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.
- b. An Apple iPhone 7, Model A1660, hereinafter "Device 2." The phone's serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369235. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PERTINENT STATUTES

Title 18, United States Code, Section 1111 (Murder) provides:

(a) Murder is the unlawful killing of a human being with malice aforethought. Every murder perpetrated by poison, lying in wait, or any other kind of willful, deliberate, malicious, and premeditated killing; or committed in the perpetration of, or attempt to perpetrate, any arson, escape, murder, kidnapping, treason, espionage, sabotage, aggravated sexual abuse or sexual abuse, child abuse, burglary, or robbery; or perpetrated as part of a pattern or practice of assault or torture against a child or children; or perpetrated from a premeditated design unlawfully and maliciously to effect the death of any human being other than him who is killed, is murder in the first degree.

Any other murder is murder in the second degree.

(b) Within the special maritime and territorial jurisdiction of the United States,

Whoever is guilty of murder in the first degree shall be punished by death or by imprisonment for life;

Whoever is guilty of murder in the second degree, shall be imprisoned for any term of years or for life.

Title 18, United States Code, Section 7(9)(B) provides that, with respect to offenses committed by or against a national of the United States, the “special maritime and territorial jurisdiction of the United States” includes residences in foreign States and the land appurtenant or ancillary thereto, irrespective of ownership, used for purposes of United States diplomatic, consular, military, or other United States Government missions or entities in foreign states, or used by United States personnel assigned to those missions or entities.

PROBABLE CAUSE

7. On September 22, 2018, Kevin L. Webb, an American diplomat serving at the American Embassy in Antananarivo, Madagascar, was found dead in his Madagascar apartment by members of the U.S. State Department’s Regional Security Office (RSO).

8. Malagasy authorities detained a suspect, Davidaso RANDRIANOTAHIANA. According to a guard at Mr. Webb's apartment, and RANDRIANOTAHIANA's statements to local authorities, RANDRIANOTAHIANA was a guest of Mr. Webb's the evening of September 21, 2018. RANDRIANOTAHIANA was seen leaving Mr. Webb's home early on September 22, 2018. He was encountered by security officials, who noticed blood on his clothing. RANDRIANOTAHIANA told security officials that he and Mr. Webb had fought. Medical personnel and Embassy personnel entered Mr. Webb's home and found him deceased.

9. Embassy personnel found the devices in a fanny pack strapped around Mr. Webb's waist. The Devices and other valuables were removed from the fanny pack by RSO personnel for safe-keeping before Mr. Webb's body was transported to the local morgue until arrangements were made for him to be transported to the United States.¹

10. Agents from DSS Office of Special Investigation, including your Affiant, were dispatched from the U.S. to Madagascar to investigate Mr. Webb's death. The RSO turned over the devices to DSS agents while they were in Madagascar, and the DSS agents brought the Devices back with them to the United States on September 29, 2018, and secured them as evidence. The contents of the Devices have thus far not been searched or reviewed.

¹ Subsequent to the removal of Mr. Webb's body from his home, a search warrant was executed at his apartment in Madagascar. The search warrant was authorized by a Magistrate Judge sitting in Washington, D.C., pursuant to Fed. R. Crim. P. 41(b)(5)(B)&(C), authorizing search warrants for U.S. diplomatic or consular premises (regardless of who owns them) or for residence and land leased by the U.S. and used by U.S. personnel assigned to a U.S. diplomatic or consular mission abroad. The Devices were no longer in Mr. Webb's apartment at the time of the execution of the search warrant.

11. DSS learned through interviews with witnesses in Madagascar that Mr. Webb may have used a real-time translation application on one of the phones to facilitate communication between himself and RANDRIANOTAHIANA the evening of September 21, 2018. DSS believes this application may have retained logs of this communication, and that such logs would shed light onto the nature of the interaction between Mr. Webb and the subject, perhaps including any motive the subject may have had for killing Mr. Webb. Further, your Affiant is aware that iPhones and SIM cards can contain GPS information, contacts, photos, files, and other items which may help determine Mr. Webb's activities and interactions the evening of his death.

12. DSS believes that Device 1 is a work phone, owned by the U.S. Department of State, and Device 2 is a personal phone.

13. The Devices are currently in storage at the DSS Office of Special Investigations in Arlington, Virginia. In my training and experience, I know that the cell phones and SIM cards have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of DSS.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

15. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, GPS navigation device and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, their location, and their time-correlated activities.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- c. The process of identifying the exact electronically stored information on storage media that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how the devices were used, the purpose of the use, who used them, and when, sometimes it is necessary to establish that a particular thing is not present on the storage media.

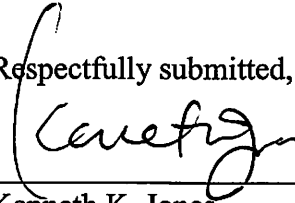
18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire media, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Kenneth K. Jones
Special Agent
Diplomatic Security Service
Office of Special Investigations

Subscribed and sworn to before me
On November 1, 2018:



/s/

Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

The property to be searched are two cell phones and the SIM cards located within each, collectively, “the Devices”:

- a. An Apple iPhone 6S, Model A1633, FCC ID BCG-E2946A bearing a sticker barcode with the number 027411, hereinafter Device 1. The phone’s serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369250. The protective case of the phone bears a sticker with the number 034 49 352 10. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.
- b. An Apple iPhone 7, Model A1660, FCC ID BCG-E3085A, hereinafter Device 2. The phone’s serial number is not available without accessing the phone. The SIM card in the phone bears the following markings: 8926104261 Telma M 4G 601369235. The Device is currently secured at the DSS Office of Special Investigations, 1800 N. Kent Street, Arlington, Virginia.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Devices described in Attachment A that relate to the victim, Kevin Webb's activities, whereabouts, and communications preceding his death, including:

- a. Any Device application that facilitates communication, particularly translated communication;
- b. any archived information related to Mr. Webb's location as recorded by the Devices' GPS;
- c. any information, such as contact information, demonstrating the nature of the relationship between Mr. Webb and the subject of investigation;
- d. any Device media which, with time-stamps, correlate Mr. Webb's location and activities in the hours preceding his death; and
- e. evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.